CERT-PH Cybersecurity Threat Feeds

Issue Date	February 24, 2021
TLP: GREEN	

Summary

The latest cyber threat topics gathered from the web and analyzed by the CERT-PH research team over the last 24 hours that may impact the Philippine government and cyberspace:

- Ukraine: DDoS Attacks on Govt Sites Originated from Russia
- Twitter Removes Accounts Linked to Russian Government-backed Actors
- VMware Addresses a Critical RCE Issue in vCenter Server
- IBM Addressed Flaws in Java Runtime, Planning Analytics Workspace, Kenexa LMS

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Ukraine: DDoS Attacks on Govt Sites Originated from Russia

2021.02.23 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Ukraine ‘s government accused unnamed Russian traffic networks as the source of massive attacks on Ukrainian security and defense websites. According to researchers, attacks were carried out on the websites of the Security Service of Ukraine, the National Security and Defense Council of Ukraine, resources of other state institutions and strategic enterprises. It was revealed that addresses belonging to certain Russian traffic networks were the source of these coordinated attacks. Investigations uncovered a new malware planted on vulnerable Ukrainian government servers that adds the devices into an attacker-controlled botnet. These devices are then reportedly used to perform further DDoS attacks on other Ukrainian sites.

Read more:

[https://www.bleepingcomputer[.]com/news/security/ukraine-ddos-attacks-on-govt-sites-originated-from-russia/]
[https://securityaffairs[.]co/wordpress/114913/cyber-warfare-2/russian-networks-ukraine-sites.html]

Twitter Removes Accounts Linked to Russian Government-backed Actors

2021.02.23 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Twitter has removed dozens of accounts used by Russia-linked threat actors that were used to disseminate disinformation and to target the European Union, the United States, and the NATO alliance. According to cybersecurity experts, the accounts were part of two separate clusters that were operated by Russian actors and that targeted different entities. A first cluster composed of 69 fake accounts, part of these accounts were used to amplify narratives that were aligned with the politics of the Russian government, while a second subset was focused on undermining faith in the NATO alliance and its stability. The second Russian-linked disinformation network was composed of 31 accounts, from two distinct networks allegedly affiliated with the Internet Research Agency (IRA) and Russian government-linked actors. The accounts were used to amplify narratives that had been previously associated with the IRA and other Russia-linked organizations. The accounts were involved in disinformation campaigns targeting the United States and European Union.

Read more:

[https://www.bleepingcomputer[.]com/news/security/twitter-removes-accounts-of-russian-government-backed-actors/]
[https://securityaffairs[.]co/wordpress/114950/social-networks/twitter-removes-russia-disinformation.html]

VMware Addresses A Critical RCE Issue In vCenter Server

2021.02.22 | Source(s): Bleeping Computer, Security Affairs

Analysis:

VMware has addressed a critical remote code execution (RCE) vulnerability in the vCenter Server virtual infrastructure management platform that could be exploited by attackers to potentially take control of affected systems. Tracked as CVE-2021-21972, the flaw affects vCenter Server plugin for vROPs which is available in all default installations and received a CVSSv3 base score of 9.8/10. When exploited successfully, malicious actors with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server.

Read more:
[https://securityaffairs[.]co/wordpress/114957/security/vmware-in-vcenter-server-rce.html]
[https://www.bleepingcomputer[.]com/news/security/vmware-fixes-critical-rce-bug-in-all-default-vcenter-installs/]

IBM Addressed Flaws in Java Runtime, Planning Analytics Workspace, Kenexa LMS

2021.02.23 | Source(s): Security Affairs, Threatpost

Analysis:

IBM has released security updates to address several high- and medium-severity flaws affecting some of its enterprise products, including IBM Java Runtime, IBM Planning Analytics Workspace, and IBM Kenexa LMS On Premise. Tracked as CVE-2020-14782 and CVE-2020-27221, are two issues that affect Runtime Environment Java 7 and 8 which is used in IBM Integration Designer. The most severe issue, tracked as CVE-2020-27221, is a stack-based buffer overflow that resides in Eclipse OpenJ9. The issue received a CVSS base score of 9.8 and could be used by remote attackers to execute arbitrary code or cause an application crash.

Read more:
[https://securityaffairs[.]co/wordpress/114942/security/ibm-security-flaws.html]
[https://threatpost[.]com/ibm-critical-remote-code-execution-flaw/164187/]

CERT-PH Recommendations:

o Update any vulnerable system/applications/devices to their latest and patched versions:
- VMware vCenter Server - versions 6.5 U3n, 6.7 U3l, and 7.0 U1c
- IBM (Java Runtime, Planning Analytics Workspace, Kenexa LMS On Premise) - latest version

o Agencies must protect their assets and perimeter by minimizing the point of entry that an unwanted attacker might take. Thus, actions must be taken such as:
- Closing misconfigured and/or unused ports that are accessible in the public internet.
- Regularly monitoring and patching of systems, software application, and devices.
- Educating employees regarding cyber hygiene and cybersecurity best practices.

Critical	*The information stated is deemed to be crucial to organizations and can significantly shift security concerns and issues based on following events.*
Urgent	*The information stated needs to be addressed timely, which may require immediate attention and/or prompt action.*
Information	*The information stated is good to know knowledge that provides awareness and understanding to the topic.*